

附件 4

信息发布审核制度

我公司已建立一套完善的信息安全审核、发布机制，具体如下：

1. 完善业务平台信息安全机制

- (1) 平台操作账号登陆业务平台时具有短信验证码功能；
- (2) 完善信息发送“敏感词”过滤与预警功能；
- (3) 未经审核的信息无法实现发送，提高信息安全把关力度。

2. 做好网站安全保障措施

(1) 物理层安全

为保证计算机信息系统各种设备的物理安全是保障整个网络系统安全的前提。物理安全是保护计算机网络设备、设施以及其它媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。它主要包括三个方面：环境安全、设备安全、线路安全。

为了将不同密级的网络隔离开，我们还采用隔离技术将核心密和普密两个网络在物理上隔离，同时保证在逻辑上两个网络能够连通。

(2) 网络层安全

防火墙技术。公司在内网和 Internet 边界安装防火墙，并实施相应的安全策略控制。另外，根据对外提供信息查询等服务的要求，为了控制对关键服务器的授权访问控制，公

司把对外公开服务器集合起来划分为一个专门的服务器子网，设置防火墙策略来保护对它们的访问。网络边界安全则采用防火墙等成熟产品和技术实现网络的访问控制，采用安全检测手段防范非法用户的主动入侵。

入侵检测系统。其能提供实时的入侵检测及采取相应的防护手段，如发现违规访问、阻断网络连接、内部越权访问等，发现更为隐蔽的攻击。公司的网络入侵安全问题将主要采用网络入侵监测系统等成熟产品和技术来解决。

数据传输安全。为保证数据传输的机密性和完整性，同时对用户接入采用强身份认证，公司将在内网中采用安全VPN系统，全面保障数据传输过程中安全准确。

(3) 系统层安全

系统层安全主要包括两个部分：操作系统安全技术以及数据库安全技术。对于关键的服务器和工作站公司将采用服务器版本的操作系统。

(4) 应用层安全

根据公司网络的业务和服务，我们采用身份认证技术、防病毒技术、以及对各种应用服务的安全性增强配置服务来保障网络系统在应用层的安全。

身份认证技术。身份认证是整个信息安全部系的基础，其能密切结合企业的业务流程，阻止对重要资源的非法访问。身份认证技术可以用于解决访问者的物理身份和数字身份的一致性问题，给其他安全技术提供权限管理的依据。

防病毒技术。随着分布式网络计算、文档驻留宏、群件

等新技术的出现以及 Internet 的广泛采用，网络的脆弱性成倍增加，保护计算机网络已不再是简单的在客户机上安装桌面病毒扫描程序就可以解决的问题了，建立一套完善多级的病毒防护系统非常必要。公司采用先进的防病毒技术，其提供了桌面、服务器和 Internet 网关的单一集成的防病毒系统，对所有潜在的病毒进入点实行全面保护。

信息安全过滤系统。公司采用公安局指定使用的信息过滤系统，该系统由公安局方面配置敏感词汇，系统认定为非法信息而会被过滤，同时将非法信息备份在公安部门的过滤系统中，保证定时刷新和监控；同时采用黑名单过滤的方式，建立并维护黑名单表，对于黑名单中用户上下行信息都进行过滤，并记入日志。

此外，公司设置远程服务器权限。网络管理员具有该用户组权限外，公司的高层领导也可以拥有该权限，由网络管理员分别设定用户名和密码。

用户权限只容许访问系统资源。该组权限分配给公司一般职员。系统管理员将设定的所有用户名和密码通知给办公室，由办公室人员进行保存，并负责保密。系统管理员修改密码或设定新的用户后，必须立即通知办公室作相应修改。

24 小时交互式信息巡查制度

加强对用户互动内容信息包括论坛、留言板等交互式栏目的有效管理，根据《网络安全法》《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》和《互联网电子公告服务管理规定》等国家法规、规章，特制定本规定：

- 1、凡所有 [REDACTED] 旗下内容板块（包括但不限于：[REDACTED]、[REDACTED]、[REDACTED]、[REDACTED]、[REDACTED] 等），相关网站、客户端公共交互信息均进行技术平台关键字过滤、屏蔽、记录相关用户 ID、IP 及发布内容，依法依规进行快速处理。
- 2、凡在 [REDACTED] 媒体版块上开办了公告栏、论坛、留言板等交互式栏目的，每个栏目均确定专人进行信息安全管理，总体设有一个安全管理总负责人；
- 3、各栏目负责信息安全管理的人员须每日定时巡查栏目内包括 FTP 上传的信息，要既巡查发布的帖子，又要仔细查看回复中出现的信息。敏感时期按有关部门的通知要求 24 小时值班巡查；
- 4、各栏目负责信息安全管理的人员若发现栏目内出现有害信息、不良信息及其他违反国家法律法规的信息，须在保存好有关记录（发贴人的 IP、发贴时间和内容等）后立即屏蔽、删除有害信息，并及时上报安全管理总负责人，必要时上报公安网安部门，同时协助有关部门查证；
- 5、安全管理总负责人每天定时对网站主页以及论坛、

留言板等交互式栏目信息进行巡查、监管；

6、对公安机关公共信息安全监察部门确定需查证的案件，各级负责信息安全管理的人员要认真协助调查，并做好详细记录，必要时须提交书面调查报告。不得拖延、推委。

网络安全应急预案

为加强集团的信息技术管理，有效保护和利用信息技术资源，最大限度的防范技术风险，确保网络宣传阵地的正常运转，根据《网络安全法》《中华人民共和国计算机信息安全保护条例》及有关法律、法规和政策，结合集团实际情况，制定本预案。

一、指导思想

不断强化政治意识、大局意识、责任意识、安全意识，高度重视网络安全，加强日常管理，做好网络安全日常监测和维护工作，及时妥善地处置影响信息安全的突发事件，为保证和维护稳定提供可靠的信息保证和良好的舆论环境。

二、工作原则

1. 统一指挥，密切协同，快速反应，科学处置。集团各部门（子公司）实行谁主管谁负责、谁运行谁负责。按各自职责划分，分级处理，层层负责。

2. 预防和处置相结合，以防为主。加强风险排查，减少故障隐患，做好应急处理各项准备，严格执行公司信息技术系统监控值守规定，确保故障及早发现。

3. 果断处理，有效应对。发现网络与信息安全事件时要紧急报告，快速启动应急预案进行处置，最大限度减少网络与信息安全事件造成的危害与影响。

三、适用范围

1. 本预案适用于集团下属各内容板块发生影响到网络

正常运行或网络信息安全，并由此可能影响到社会、国家安全稳定的事情。

2. 影响或破坏网络运行及网络信息安全的事件可分为网络安全事件和网络信息安全事件两类：网络安全事件主要指网络实体中线路、网络设备、服务器设备等出现的被病毒和恶意攻击带来的安全事件；网络信息安全事件主要指网络中各信息服务设备中出现的信息安全事件，如非法信息、泄密事件等。

3. 本预案包括集团内网和外网服务器上的各种信息服务在内。

四、应急准备

1. 系统管理员、网络管理员及各信息系统使用人员、值班人员等关键岗位应熟练掌握应急预案，确保能够有效应对信息安全事件。

2. 与相关单位签订通信、消防、电力设备、空调设备、软硬件产品的应急及服务保障协议，确保在应急处置中相关单位能够及时有效的提供技术支持。

3. 储备一定数量的通信、消防、电力、照明等设备或者物资以及其他重要备件，确保应急处置中应急物资的及时供应。

4. 应急预案相关工作人员必须保持 24 小时联络通讯畅通。

五、网站与信息安全应急措施

（一）网站、网页出现非法言论时的紧急处置措施

- 1、网站、网页由内容部门人员随时密切监视信息内容。
- 2、发现网站出现非法信息或者内容被篡改，视情况的严重程度，负责人员应立即向技术部、部门负责人、主管领导、上级主管单位，逐级汇报情况，如有必要，应立即向公安机关报警。情况紧急的应先将非法信息或篡改信息从网络中隔离出来，重新生成正确内容并上传。
- 3、技术人员在接到通知后，视情况的严重程度，依次采取以下措施：立即清理非法信息，保护现场，保存非法信息或页面，停止被篡改网站的内容服务，断开网络服务器。
- 4、网站维护员应同时作好必要的记录，追查非法信息来源，清理或修复非法信息，妥善保存有关记录，强化安全防范措施，并将网站重新投入运行，必要时请求网络安全技术服务提供方提供技术支持。

（二）黑客攻击或服务器遭破坏性攻击时的紧急处置措施

- 1、服务器系统文件、重要的配置文件应进行有效备份，当服务器系统发生故障或遭到破坏时，应立即启动备份系统对服务器操作系统及数据库进行修复和还原，保证服务器的正常运行。
- 2、当发现网页内容被篡改，或通过入侵检测系统发现有黑客正在进行攻击时，应马上通知技术部；软件遭破坏性攻击时要将系统停止运行。
- 3、技术人员迅速进行响应处理，将被攻击的服务器等设备从网络中隔离出来，同时向领导汇报情况。

4、技术部负责进行被破坏系统的恢复与重建工作，尽可能恢复数据，必要时请求网络安全技术服务提供方提供技术支持。

5、如有必要，技术人员应根据系统日志和其他信息追查非法信息来源（或攻击来源），将有关情况向相关领导汇报，强化安全防范措施。

6、妥善保存相关记录、日志和系统文件。

（三）局域网内发生病毒传播时的处置措施

1、当局域网发生病毒传播时，应立即通知技术部。技术部迅速查找病毒感染源，同时将被感染电脑设备从网络上隔离出来并对该设备的硬盘数据备份及设备系统彻底重装。

2、技术部负责升级网络防病毒软件的版本，并使用有效的病毒查杀软件对局域网计算机进行病毒扫描和清除工作。必要时请求网络安全技术服务提供方提供技术支持。

3、妥善保存相关记录、日志和系统文件。

（四）软件系统遭受破坏性攻击时的紧急处置措施

1、重要的软件系统平时必须存有备份，与软件系统相对应的数据应有多份备份，并将它们保存于安全处。

2、一旦软件系统遭到破坏性攻击，应立即向技术人员、部门负责人报告，并将系统停止运行。

3、网站技术人员立即进行软件和数据的恢复和修补工作。必要时请求软件开发方或网络安全技术服务提供方提供技术支持。

4、技术人员检查日志等资料，如有必要，应确认攻击

来源。将有关情况向相关领导或主管部门汇报。

5、妥善保存相关记录、日志和系统文件。

(五) 数据库安全紧急处置措施

1、各数据库系统要至少准备两个以上数据库备份，平时一份放在机房，另一份放在另一安全的建筑物中。

2、一旦数据库崩溃，应立即向技术人员报告。

3、系统修复启动后，技术人员迅速对数据库数据进行维护，如无法正常维护，采取数据库备份恢复。

4、如果备份均无法恢复，应立即向有关厂商寻求紧急技术支援。

(六) 服务器设备安全紧急处置措施

1、服务器等关键设备损坏后，有关人员应立即向技术人员报告。

2、技术人员应立即查明原因。如果能够自行恢复，应立即用备件替換受损部件，或使用备用服务器提供网站服务。

3、如果不能自行恢复的，立即与设备提供商联系，请求派维修人员前来维修。

4、如果设备一时不能修复，应向领导汇报。

(七) 网络线路中断或网络设备故障时的紧急处置措施

1、网络线路中断或网络硬件设备发生故障，技术人员接到报告后，应派网络维护人员迅速判断故障节点，查明故障原因，并及时予以恢复。

2、如线路中断属运营商造成的，应立即与运营商维护部门取得联系，要求恢复。

3、如果发生故障的网络设备故障一时无法修复的，应启用备份线路或者备份设备及时予以恢复。

4、如因备件损坏或其他原因，网络线路无法及时修复的，应向相关领导汇报情况。

（八）外部电源中断后的应急预案

1、外部电源中断后，应迅速切换电源，使用发电机供电 UPS，同时查明原因，通知物管检查线路。

2、UPS 负载有限，只启用机房中的关键服务器和网络设备。

3、如是提前通知的停电，事先通知各部门，做好数据的保存。

4、供电恢复后，记录恢复时间，通知部门主管，关闭发电机，将电源切回到正常的交流电，启动所有服务器，网络设备。

（九）由集团总编室负责接收相关主管部门下发的紧急处置指令，收到后应立即通知相关编辑部门进行处置，编辑部门无法处置的内容，应由编辑部门向技术部门提出处置请求，技术部门应即刻处置。

（十）、日志留存管理

为了加强网站网络的安全保护，保留可追溯的完整日志文件，维护网站网络正常运行，特制订本制度。

1、网络上的所有服务器，都进行用户权限划分，必须是具有合法权限的用户才能进行相应权限范围内的操作，任何其他非法操作都属于入侵行为，并将操作记录入日志文件。

2、指定专门的技术人员，检查日志是否正常留存并对日志进行分析，确认网站是否有被攻击以及编辑在操作内容管理系统时有无违规。

3、日志分为：应用程序日志、安全日志、系统日志、IIS 业务访问日志、内容管理系统操作日志。

4、所有日志保留时间不少于 3 个月。超过 3 个月的日志必须保存到指定的日志服务器上。只有网络信息安全管理員在主管领导授权的情况下，才能对日志进行删除处理。

用户个人信息保护制度（试行）

根据中华人民共和国《网络安全法》有关规定，为有效保护用户信息安全，建立健全 [REDACTED] 旗下各媒体版块用户信息保护制度，制定本制度。

一、个人信息：是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

二、适用范围：本制度适用于 [REDACTED] 旗下各内容板块，包括但不限于 [REDACTED]、[REDACTED]、[REDACTED]、[REDACTED]、[REDACTED]、[REDACTED] 等。

三、收集、使用个人信息，必须经过用户同意，遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围。

四、不收集与其提供的服务无关的个人信息，不违反法律、行政法规的规定和双方的约定收集、使用个人信息，依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

五、对用户身份信息和日志信息负有保密的义务，不泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不向他人提供个人信息。下列情况除外：（1）经过处理无法识别特定个人且不能复原的。（2）事先获得用户的明确授权。（3）依法配合相关单位的调查取证，如符合法律法规要求

的相关司法文书。

六、如需收集用户信息，必须采取技术措施和其他必要措施，确保收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况下，会立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

七、用户发现 [REDACTED] 旗下媒体违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求删除其个人信息；发现收集、存储的其个人信息有错误的，有权要求予以更正。并立即采取措施予以删除或者更正。

八、任何个人和组织不得窃取或者以其他非法方式获取个人信息。不得泄露、篡改、毁损，不得出售或非法向他人提供。

九、[REDACTED] 相关工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

十、任何部门或个人发布信息时，应当对其行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

十一、[REDACTED] 内容部门加强对用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，要立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存

有关记录，并向有关主管部门报告。

十二、任何个人和组织发布的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。[]依法履行安全管理义务，知道用户有前款规定行为的，将停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

十三、[]依法配合网信部门和有关部门依法实施的监督检查，网信部门和有关部门依法履行对旗下各媒体的网络信息安全监督管理职责。收到管理部门通知下发的法律、行政法规禁止发布或者传输的信息的，应停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应通知有关机构采取技术措施和其他必要措施阻断传播。

相关技术保障措施的情况

1. 网络与信息安全保障措施

(1) 在网站的服务器及工作站上均安装了防病毒软件，对计算机病毒、有害电子邮件有整套的防范措施，防止有害信息对网站系统的干扰和破坏。

(2) 做好网站访问日志的留存。网站具有保存60天以上的系统运行日志和用户使用日志记录功能，内容包括IP地址及使用情况，主页维护者、邮箱使用者和对应的IP地址情况等。

(3) 交互式栏目具备有IP地址、身份登记和识别确认功能，对没有合法手续和不具备条件的电子公告服务立即关闭。

(4) 网站信息服务系统建立了实时备份机制，一旦主系统遇到故障或受到攻击导致不能正常运行，保证备用系统能及时替换主系统提供服务。

(5) 关闭网站系统中暂不使用的功能，及相关端口，并及时用补丁修复系统漏洞，定期查杀病毒。

(6) 服务器平时处于锁定状态，并保管好登录密码；后台管理界面设置超级用户名及密码，并绑定IP，以防他人登入。

(7) 网站提供集中式权限管理，针对不同的应用系统、终端、操作人员，由网站系统管理员设置共享数据库信息的访问权限，并设置相应的密码及口令。不同的操作人员设定不同的用户名，且定期更换，严禁操作人员泄漏自己的口令。

对操作人员的权限严格按照岗位职责设定，并由网站系统管理员定期检查操作人员权限。

(8) 电信机房标准建设，内有必备的独立UPS不间断电源、定期检查灭火器。

(9) 机房配备有软、硬件防火墙，并有工作人员24小时值班。

2.信息安全管理

(1) 信息监控制度

a) 网站信息必须在网页上标明来源；(即有关转载信息都必须标明转载的地址)

b) 相关责任人定期或不定期检查网站信息内容，实施有效监控，做好安全监督工作；

c) 不得利用国际互联网制作、复制、查阅和传播一系列以下信息，如有违反规定有关部门将按规定对其进行处理；

- 违反宪法所确定的基本原则的；
- 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- 损害国家荣誉和利益的
- 煽动民族仇恨、民族歧视、破坏民族团结的；
- 破坏国家宗教政策，宣扬邪教和封建迷信的；
- 散布谣言，扰乱社会秩序，破坏社会稳定的；
- 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- 侮辱或者诽谤他人，侵害他人合法权益的；含有法

律、行政法规禁止的其他内容的。

(2) 组织结构

设置专门的网络管理员，并由其上级进行监督、凡向国际互联网的站点提供或发布信息，必须经过保密审查批准。保密审批实行部门管理，有关单位应当根据国家保密法规，审核批准后发布、坚持做到来源不明的不发、未经过上级部门批准的不发、内容有问题的不发、的三不发制度。对网站管理实行责任制对网站的管理人员，以及领导明确各级人员的责任，管理网站的正常运行，严格抓管理工作，实行谁管理谁负责。因疏于管理而导致网络安全事故和信息管理事故的，将追究该单位网络工作主管领导、信息监控人员、网络管理员的责任，视事故严重程度给予相关责任人以行政处罚。

3. 用户信息安全管理

(1) 信息安全内部人员保密管理制度：

- a) 相关内部人员不得对外泄露需要保密的信息；
- a) 内部人员不得发布、传播国家法律禁止的内容；
- b) 建立信息发布审核机制，信息发布之前经过相关人员审核；
- c) 对相关管理人员设定网站管理权限，不得越权管理网站信息；
- d) 一旦发生网站信息安全事故，应立即报告相关方并及时进行协调处理；
- e) 对有毒有害的信息进行过滤、用户信息进行保密。

(2) 登陆用户信息安全管理

- a) 登记注册表应由专人负责保管，未经授权不得复制、透露给第三方；
- b) 只允许用户的单一登录；即单一用户名只对应单一口令
- c) 对登陆用户信息阅读与发布按需要设置权限。用户可自主改变登录密码，以保护用户信息的隐私权；
- d) 对用户在网站上的行为进行有效监控，保证内部信息安全；
- e) 规定用户不得传播、发布国家法律禁止的内容。
- f) 针对用户发布信息建立审核机制，设定信息开关，所有信息一律律师事务所审核后再开放显示。
- g) 除用户授权外，系统管理员不得对用户信息进行复制、更改；
- h) 定期将用户信息备份并保存，以防用户误操作，丢失原有信息；
- i) 加强对用户的网络制度、法律法规的宣传；并组织集中学习与培训，加强用户相关的法律意识，提高用户的自我约束能力。
- j) 固定用户不得传播、发布国家法律禁止的内容。
- k) 如用户要求对服务器网络配置进行改动、增减信息目录结构，用户需要向系统分析员提出书面申请。